

































-  Secrets
-  ABAP
-  Apex
-  C
-  C++
-  CloudFormation
-  COBOL
-  C#
-  CSS
-  Flex
-  Go
-  **HTML**
-  Java
-  JavaScript
-  Kotlin
-  Kubernetes
-  Objective C
-  PHP
-  PL/I
-  PL/SQL
-  Python
-  RPG
-  Ruby
-  Scala
-  Swift
-  Terraform
-  Text
-  TypeScript
-  T-SQL
-  VB.NET
-  VB6
-  XML



HTML static code analysis

Unique rules to find Bugs, Security Hotspots, and Code Smells in your HTML code

All rules 65

Bug 24

Security Hotspot 3

Code Smell 38

Tags ▾

Search by name... 🔍

Table cells should reference their headers	Bug
Tables used for layout should not include semantic markup	Bug
Tables should have headers	Bug
"<html>" element should have a language attribute	Bug
<script>...</script> elements should not be nested	Bug
"<th>" tags should have "id" or "scope" attributes	Bug
"<title>" should be present in all pages	Bug
"<!DOCTYPE>" declarations should appear before "<html>" tags	Bug
Elements deprecated in HTML5 should not be used	Bug
HTML "<table>" should not be used for layout purposes	Code Smell
"aria-label" or "aria-labelledby" attributes should be used to differentiate similar elements	Code Smell
Videos should have subtitles	Code Smell
Attributes deprecated in HTML5 should not be used	Code Smell
Sections of code should not be commented out	

Disabling resource integrity features is security-sensitive

Analyze your code

Security Hotspot Minor ? cwe owasp

Fetching external resources, for example from a CDN, without verifying their integrity could impact the security of an application if the CDN gets compromised and resources are replaced by malicious ones. Resources integrity feature will block resources inclusion into an application if the pre-computed digest of the expected resource doesn't match with the digest of the retrieved resource.

Ask Yourself Whether

- The resources are fetched from external CDNs.

There is a risk if you answered yes to this question.

Recommended Secure Coding Practices

- implement resources integrity checks for all static resources (where "static" means that the resource's content doesn't change dynamically based on the browser)
- use versioned resources instead of using "latest" version of the resources

Sensitive Code Example

```
<script src="https://cdnexample.com/script.js"></script> <!--
```

Compliant Solution

```
<script src="https://cdnexample.com/script.js" integrity="sha
```

See

- [OWASP Top 10 2021 Category A8](#) - Software and Data Integrity Failures
- [MITRE, CWE-353](#) - Missing Support for Integrity Check
- [OWASP Top 10 2017 Category A6](#) - Security Misconfiguration
- [developer.mozilla.org](#) - Subresource Integrity

Available In:

sonarcloud | sonarqube

<div> Code Smell</div>
<div>Track uses of "FIXME" tags</div> <div><div> Code Smell</div></div>
<div>Meta tags should not be used to refresh or redirect</div> <div><div> Code Smell</div></div>
<div>Links should not directly target images</div> <div><div> Code Smell</div></div>
<div>"" and "" tags should be used</div> <div><div> Bug</div></div>
<div>"" and "<dt>" item tags should be in "", "" or "<dl>" container tags</div> <div><div> Bug</div></div>
<div>Server-side image maps ("ismap" attribute) should not be used</div> <div><div> Bug</div></div>
<div>"<frames>" should have a "title" attribute</div> <div><div> Bug</div></div>
<div>"<fieldset>" tags should contain a "<legend>"</div> <div><div> Bug</div></div>
<div>Flash animations should be embedded using both "<object>" and "<embed>"</div> <div><div> Bug</div></div>